<u>AMENDMENTS TO THE CLAIMS</u>

The Claims are pending as follows:

1. (Previously Presented)   A system for tracking location of a wireless device, the system comprising:

a system data store capable of storing one or more tracking criteria and indicators of one or more wireless devices to track;

a set of one or more wireless receivers on one or more wireless sensors;

a system processor in communication with the system data store and the one or more wireless sensors, wherein the system processor comprises one or more processing elements programmed or adapted to perform the steps comprising of:

(a) identifying a wireless device for tracking based upon a combination of dynamic operational and security assessments derived using data from the system data store, wherein the dynamic operational and security assessments identify the wireless device for tracking responsive to behavior of the wireless device, wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings, and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings;

(b) receiving data from a subset of the one or more wireless sensors;

(c) storing the received data in the system data store, wherein the received data is utilized to update wireless statistics used in the dynamic operational and security assessments, wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior;

(d) calculating the position of the identified wireless device based upon the stored data; and

(e) outputting the calculated position.

2. (Original)   The system of claim 1, wherein one or more tracking criteria are of a type selected from the group consisting of time, traffic level, threat level, protocol characteristics, usage characteristics or combinations thereof.

3. (Original)   The system of claim 1, wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of dynamically determining one or more tracking criteria.

4. (Original)   The system of claim 1, wherein the one or more processing elements of the system processor are further programmed or adapted to the step comprising of (f) repeat steps (a) through (e) continuously.

5. (Original)   The system of claim 1, wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) repeating steps (a) through (e) periodically.

6. (Original)   The system of claim 5, wherein the one or more processing elements of the system processor are further programmed or adapted to the step comprising of (g) modifying the period of repetition of step (f) based upon one or more tracking criteria.

7. (Original)   The system of claim 6, wherein each of the one or more tracking criteria are selected from the group consisting of time, traffic level, threat level, protocol characteristics, usage characteristics or combinations thereof.

8. (Original)   The system of claim 1, wherein the programming or adaptation to identify the wireless device includes programming or adaptation to perform the step comprising of

selecting the identified wireless device based upon indicators of one or more wireless devices in the system data store.

9. (Original)   The system of claim 8, wherein the one or more processing elements of the system processor are further programmed or adapted to perform the steps comprising of (f) detecting an unauthorized wireless device and (g) storing an indicator of the unauthorized wireless device in the system data store.

10. (Original) The system of claim 9, wherein the identified wireless device is the unauthorized wireless device.

11. (Original) The system of claim 8, wherein the programming or adaptation to identify the wireless device includes further programming or adaptation to perform the step comprising of retrieving indicators of one or more wireless devices from the system data store.

12. (Original) The system of claim 1, wherein the programming or adaptation to calculate the position of the identified wireless device includes programming or adaptation to perform the steps comprising of:

(i) sensing the identified wireless device;

(ii) storing RF signal characteristics in the system data store based upon the sensing; and

(iii) dynamically selecting one or more additional sensors to improve tracking performance.

13. (Original) The system of claim 1, wherein the programming or adaptation to output the calculated position includes programming or adaptation to perform the steps comprising of formatting the calculated position according to one or more output preferences.

14. (Original) The system of claim 13, wherein the calculated position for output is

formatted as an e-mail, a web page, a facsimile, a graphic, an XML page, an SNMP message, a page, or combinations thereof.

15. (Original) The system of claim 1, wherein the calculated position is output to a user or to a computer system.

16. (Original) The system of claim 1, wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) storing the calculated position in the system data store.

17. (Original) The system of claim 1, wherein the one or more processing elements of the system processor are further programmed or adapted to perform the step comprising of (f) removing an indicator of a wireless device from the system data store.

18. (Original) The system of claim 17, wherein indicator removal is based upon manual deletion, timed deletion, or a change in device security status from unauthorized to authorized.

19. (Previously Presented)   A method for tracking location of a wireless device, the method comprising the steps of:

     (a) detecting a wireless device utilizing one or more dynamic operational and security assessments, wherein the one or more dynamic operational and security assessments detect the wireless device responsive to behavior of the wireless device, and wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings, and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings;

(b) adding an indicator associated with the detected wireless device to a list of wireless devices;

(c) selecting a wireless device for tracking based upon the list of wireless devices;

(d) receiving data from one or more wireless sensors, wherein received data is utilized to update wireless statistics used in the dynamic operational and security assessments, wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior;

(e) calculating a position of the selected wireless device based upon the received data;

(f) outputting the calculated position;

(g) repeating steps (a) and (b) upon occurrence of an event or at periodic intervals;

(h) repeating steps (c) through (f) upon occurrence of an event or at periodic intervals.

20. (Previously Presented)   One or more computer readable media storing instruction that upon execution by a system processor cause the system processor to perform the method of claim 19, and wherein the system processor comprises a distributed processor distributed between the one or more wireless sensors and a host system.

21. (Previously Presented)   A system for tracking location of a wireless device, the system comprising:

storing means for storing one or more tracking criteria and indicators of one or more wireless devices to track;

one or more wireless sensors for scanning wireless traffic;

distributed rogue detection means for detecting a wireless device based upon one or more dynamic operational and security assessments operable to detect the wireless device based on behavior, wherein the assessments are performed on the received scan data, and for storing an indicator of the detected wireless device, wherein the distributed rogue detection means is distributed between the one or more wireless sensors and a host system; and

position determining means for selecting a wireless device to track from the indicators in the storing means, receiving scan data from one or more wireless receivers, estimating the position of the selected wireless device based upon received scan data and outputting the estimated position;

wherein the dynamic operational and security assessments comprise wireless signature-based tests, wireless protocol-based tests, wireless anomaly-based tests, and wireless policy deviation-based tests, and wherein the policy deviation-based tests ensure the wireless device is complying with the one or more wireless policy settings;

wherein the policy deviation-based tests comprise a deviation from a set of one or more wireless policy settings comprising wireless channel settings, authentication settings, encryption settings, SSID broadcast settings, and rate settings; and

wherein received scan data is utilized to update wireless statistics used in the dynamic operational and security assessments, and wherein the wireless statistics enable the dynamic operational and security assessments to detect both unauthorized wireless devices and authorized wireless devices which are displaying anomalous behavior.